



AF *[Handwritten signature]*

Attorney's Docket No. 003022.P019X

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application of:

Vance C. Bjorn

Application No.: 09/707,417

Filed: November 6, 2000

For: A Method And Apparatus For Using A
Third Party Authentication Server

Examiner: Aravind K. Moorthy

Art Unit: 2131

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPELLANT'S BRIEF TRANSMITTAL

Sir:

Enclosed for consideration is Appellant's Appeal Brief pursuant to C.F.R. §41.37 for the above-referenced case. This Brief is submitted in response to the Final Office Action mailed by the Examiner on June 17, 2004.

If there are any additional charges, please charge Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN

Dated: 1/18, 2005

[Handwritten signature]

Judith A. Szepesi
Reg. No. 39,393

12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025-1026
(408) 720-8300

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail with sufficient postage in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450 on January 18, 2005.

(Date of Deposit)

Judith Szepesi

(Typed or printed name of person mailing correspondence)

(Signature of person mailing correspondence)



003022.P019X

Patent

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application of:

Vance C. Bjorn

Application No: 09/707,417

Filing Date: November 6, 2000

For: A Method And Apparatus For
Using A Third Party Authentication
Server

Examiner: Aravind K. Moorthy

Art Unit: 2131

Confirm. No. 9958

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

Sir:

Appellant hereby submits this Brief in support of its appeal from a final decision by the Examiner, dated June 17, 2004, in the above-captioned case. Appellant respectfully requests consideration of this appeal by the Board of Patent Appeals and Interferences for allowance of the above-captioned patent application. This Appeal Brief is hereby submitted pursuant to 37 C.F.R. § 41.37(a).

An oral hearing is not desired.

01/25/2005 CNGUYEN 00000022 09707417

01 FC:1402

500.00 OP

TABLE OF CONTENTS

I.	REAL PARTY IN INTEREST	3
II.	RELATED APPEALS AND INTERFERENCES	3
III.	STATUS OF THE CLAIMS	3
IV.	STATUS OF AMENDMENTS.....	3
V.	SUMMARY OF CLAIMED SUBJECT MATTER.....	4
VI.	GROUND OF REJECTION TO BE REVIEWED ON APPEAL	7
VII.	ARGUMENTS	8
	A. Claims 1, 5, 6, 8, 9, 11-14, 17, 23, 24, 26, 27 and 29-31 are Patentable under 35 U.S.C. §102(e) over U.S. Patent No. 6,151,676 issued to Cuccia, et al.	8
	B. Claims 2-4 and 20-22 are Patentable under 35 U.S.C. §103(a) over Cuccia, et al. as applied to claim 1 above, and further in view of U.S. Patent No. 6,233,685 issued to Smith, et al.	12
	C. Claims 7, 10, 25 and 28 are Patentable under 35 U.S.C. §103(a) over Cuccia, et al. as applied to claim 1 above, and further in view of U.S. Patent No. 6,581,161 issued to Byford.	12
	D. Claims 15, 16, 18 and 21 are Patentable under 35 U.S.C. §103(a) over Cuccia, et al. as applied to claims 14 and 17 above, and further in view of U.S. Patent No. 5,692,106 issued to Towers, et al.	13
	E. Claims 19 and 22 are Patentable under 35 U.S.C. §103(a) Cuccia, et al. as applied to claim 17 above, and further in view of U.S. Patent No. 6,119,227 issued to Mao.	15
VIII.	CONCLUSION	17
IX.	APPENDIX OF CLAIMS.....	18

I. REAL PARTY IN INTEREST

The invention is assigned to DigitalPersona, Inc., of 720 Bay Road, Suite 100 Redwood City, CA 94063.

II. RELATED APPEALS AND INTERFERENCES

To the best of Appellant's knowledge, there are no appeals or interferences related to the present appeal that will directly affect, be directly affected by, or have a bearing on the Board's decision.

III. STATUS OF THE CLAIMS

Claims 1-31 are currently pending in the above-referenced application. Claims 1-31 were rejected in the Final Office Action mailed on June 17, 2004, and are the subject of this appeal.

IV. STATUS OF AMENDMENTS

In response to the Final Office Action mailed June 17, 2004, rejecting claims 1-31, Appellant filed an Amendment After Final under 37 C.F.R. 1.116 on August 17, 2004, and received an Advisory Action mailed October 1, 2004, refusing to enter the Amendment After Final. Appellant filed a Notice of Appeal on November 17, 2004.

A copy of all claims on appeal is attached hereto as an Appendix.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Appellant's invention as claimed in claims 1-31 discusses method and apparatus for a third party authentication server is described. The authentication server described herein enables web services to provide a third party authentication option to their users. For one embodiment, this authentication relies on biometrics. For one embodiment, users use a fingerprint sensor, install it on their system, and within minutes register their fingerprint to access websites. Many institutions, including banking, financial, healthcare, corporate, and government Intranets and Extranets can benefit from this secure and convenient user authentication mechanism. The system may further be used to unlock a smart card or other secured system. This system is transparent to the user, maintains user privacy, ensures the utmost security of the process, and makes the service very easy to deploy and administer by web services and their customers. (page 5, lines 2-14).

A client 210 is connected to a server 240 (such as a bank, or other destination) through a network 230 (such as the Internet). If the client 210 wants to log into a secure site on the server 240, the client is prompted by the server 240 to enter the authentication data (such as a password, or biometric information). Instead of responding directly to the server 240, the user's authentication data -- in one embodiment biometric data -- is sent by the user's system to the authentication server 220, along with a record ID associated with the particular secure site to which the user is attempting to connect. (page 5, lines 15-20).

In one embodiment, the authentication server 220 then uses the record ID to determine whether the authentication data matches the registered user for the secure site. If the user is successfully authenticated, the requested cryptographic function is provided by the authentication server 220. (page 6, lines 1-5).

In response to this request, the website sends login page to present the logon options. The client 240 initiates a session with the authentication server. (message 3). For one embodiment, the session is initiated via HTTPS, or another secure mechanism. For one embodiment, this process is driven by a client authentication object. (page 17, lines 1-14).

For one embodiment, the client authentication object raises event to indicate that it is ready. The logon page alerts the user that the fingerprint sensor is ready. The user performs the biometric authentication. For one embodiment, the user places the finger on the sensor, to use a fingerprint. (page 17, lines 20-24).

In response to receiving the client user name, the web service 230 generates a challenge. The web service sends the record ID associated with the username, the encrypted challenge, and the policy to the client. (page 18, lines 4-17). The client object forwards the record ID, encrypted challenge, and if appropriate the policy, to the authentication server. The client object also sends the encrypted biometric template to the authentication server. (page 19, lines 9-11).

The authentication server 220 compares the biometric template received from the client 240 against the template associated with the record ID. The authentication server 220 then determines if the policy requires additional data. For example, the policy may require multiple biometric matches to authenticate. The authentication server 220 follows the policy defined by the web server 230, and only declares a match if all the data necessary for a match has been obtained. If a valid match is found, the authentication server 220 decrypts the challenge with the private key 525 associated with that record ID. (block 10).

The authentication server sends the decrypted challenge to the client object. (message 11). For one embodiment, as discussed above, this occurs over a secure

channel. For one embodiment, the decrypted challenge is encrypted with the partner key.

The client object passes the challenge on to the web service (message 12). The web service compares the challenge received to the challenge sent (block 13). If the challenges match, and all other aspects of the policy have been satisfied, the web service permits the user to access the partner. At this point, the user has been successfully validated. (page 19, line 12 to page 20, line 3)

During set-up, an anonymous record is created for the user. The anonymous record includes the user's biometric data. This enables anonymous, but fully identifiable user identities. A record ID is generated for the anonymous record. For one embodiment, the record ID is generated randomly. For another embodiment, record IDs may be sequential, or may be generated using some other mechanism.

A public/private key pair is also generated for the client. For one embodiment, the public/private key pair may be a maximum length. For another embodiment, multiple key pairs may be generated. (page 21, lines 1-9). An entry is created in the credential database. The entry is indexed by the record ID, and includes the biometric template(s) and the private key(s) of the user. (page 21, lines 14-16).

VI. GROUND OF REJECTION TO BE REVIEWED ON APPEAL

Whether 1, 5, 6, 8, 9, 11-14, 17, 23, 24, 26, 27 and 29-31 are anticipated under 35 U.S.C. §102(e) over U.S. Patent No. 6,151,676 issued to Cuccia, et al.

Whether claims 2-4 and 20-22 are obvious under 35 U.S.C. §103(a) over U.S. Patent No. 6,151,676 issued to Cuccia, et al. and further in view of U.S. Patent No. 6,233,685 issued to Smith, et al.

Whether claims 7, 10, 25 and 28 are obvious under 35 U.S.C. §103(a) over U.S. Patent No. 6,151,676 issued to Cuccia, et al. and further in view of U.S. Patent No. 6,581,161 issued to Byford.

Whether claims 15, 16, 18 and 21 are obvious under 35 U.S.C. §103(a) over U.S. Patent No. 6,151,676 issued to Cuccia, et al. and further in view of U.S. Patent No. 5,692,106 issued to Towers, et al.

Whether claims 19 and 22 are obvious under 35 U.S.C. §103(a) over U.S. Patent No. 6,151,676 issued to Cuccia, et al. and further in view of U.S. Patent No. 6,119,227 issued to Mao.

VII. ARGUMENTS

Appellant respectfully submits that all the appealed claims in this application are patentable over the combination of cited references suggested by the Examiner.

A. Claims 1, 5, 6, 8, 9, 11-14, 17, 23, 24, 26, 27 and 29-31 are Patentable under 35 U.S.C. §102(e) over U.S. Patent No. 6,151,676 issued to Cuccia, et al.

Examiner rejected claims 1, 5, 6, 8, 9, 11-14, 17, 23, 24, 26, 27 and 29-31 under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,151,676 issued to Cuccia, et al. (hereinafter Cuccia).

Cuccia discusses a public key cryptosystem employing El-Gamal algorithm. The portion reference by the Examiner, column 6, lines 13-49 discuss how passphrase or biometric data is used to generate a user identifying key, which is then used to encrypt the user's private key. However, the passphrase or biometric information is immediately deleted from the system once the private key is encrypted. (Cuccia, column 7, lines 13-15). The "user identifying key" is a temporary construct in Cuccia. The Examiner asserts that the "user identifying key" of Cuccia is equivalent to the record ID of the present invention. Appellants respectfully disagree with this analysis. The "user identifying key" or KPAS of Cuccia is a hash of the user's biometric data (Cuccia, column 7, lines 5-15). This KPAS information is used to encrypt the user's key, and then discarded. The KPAS or "user identifying key" IS the user's authentication data. On a subsequent occasion, when the user logs in, the user's biometric data is used to recreate the KPAS.

In contrast, claim 1 of the present invention recites:

A method of authenticating a client, the method comprising in an authentication server:
receiving a record ID for a user, and a one-time key generated by a third party server and encrypted with a user's public key by the server;
receiving the user's authentication data from the client;
determining if the user's authentication data matches the record ID; and
if so, decrypting the one-time key with the user's private key, and returning the decrypted one-time key to the client.

The record ID, as claimed, is an identifier associated with the particular secure site to which the user is attempting to connect. (page 5, lines 15-20). It is not the user's biometric, nor is it related to the user's authentication data. It is not "user identifying data" but rather secure site identifying data, identifying the secure site to which the user is attempting to provide authentication. Furthermore, in Cuccia, the "user identifying key" or KPAS is generated by the server, rather than received by the server from an external source. (See Cuccia, column 7, lines 30-31). Thus, Cuccia does not teach or suggest receiving a record ID, as claimed in claim 1.

Therefore, Appellants respectfully submit that claim 1, and its dependent claims 2-13 are not anticipated by Cuccia.

Similarly, independent claim 17 recites in part "an authentication server to receive a record ID for a user, and a one-time key generated by a third party server and encrypted with a user's public key by the third party server." Therefore, for the same reasons advanced above regarding "record IDs" Cuccia does not anticipate claim 17, and its dependent claims 18-31.

A2. Claims 11-13 and 29-31

Examiner rejected claims 11-13 and 29-31, under 35 U.S.C. §102(b) as being unpatentable over Cuccia. These claims incorporate the limitations of their parent claims, and thus also recite “receiving a record ID.” Therefore, for at least the reasons discussed above Cuccia does not anticipate these claims.

Furthermore, claim 11, on which claims 12-13 depend, recites:

The method of claim 1, wherein the record ID and the encrypted one-time key are further encrypted using a partner key, the method further comprising decrypting the record ID and encrypted one-time key using the partner key.

Cuccia does not teach or suggest interacting with a third party, in addition to the user for encryption and authentication. Therefore, Cuccia does not teach or suggest the use of encrypting data with a partner key. The Examiner suggests that column 10, lines 15-55 of Cuccia shows this feature. This section of Cuccia discusses what occurs once the user has been successfully authenticated. It has nothing to do with what data is received, and used as part of the authentication process. Appellant fails to see any reference to a partner key, in any case.

Note that the encrypted data is encrypted by the third party server, but sent to the authentication server by the client (user).

Similarly, claim 29, on which claims 30-31 depend, recites in part “wherein the decryption logic further decrypts the record ID and the encrypted one-time key with a partner key.” As noted above, Cuccia does not teach or suggest a partner key.

Since Cuccia does not teach or suggest such a partner key, the claims of Group II are not anticipated by Cuccia.

A3. Claims 14-16

Examiner rejected the claims 14-16, under 35 U.S.C. §102(b) as being unpatentable over Cuccia. These claims incorporate the limitations of their parent claims, and thus also recite “receiving a record ID.” Therefore, for at least the reasons discussed above Cuccia does not anticipate these claims. Furthermore, claim 14, on which claims 15-16 depend, recites:

A method of using an authentication server to authenticate a user to a third party server, the method comprising the third party server:
looking up a record ID associated with the user;
generating a one-time key and encrypting the one-time key with a public key of the user, and sending the encrypted one-time key and the record ID to the user;
receiving authentication data, the authentication data being the decrypted one-time key decrypted with the user's private key by the authentication server, such that the user does not have control of the user's private key at any time; and
permitting access to the server.

Cuccia does not teach or suggest a third party server looking up a record ID associated with the user. In fact, Cuccia does not teach or suggest the use of a third party server in connection with the authentication function. Furthermore, as noted above, Cuccia does not teach or suggest the use of record IDs. Therefore, claims 1-14 are not anticipated by Cuccia.

B. Claims 2-4 and 20-22 are Patentable under 35 U.S.C. §103(a) over Cuccia, et al. as applied to claim 1 above, and further in view of U.S. Patent No. 6,233,685 issued to Smith, et al.

Examiner rejected claims 2-4 and 20-22 under 35 U.S.C. §103(a) as being unpatentable over Cuccia, et al. as applied to claim 1 above, and further in view of U.S. Patent No. 6,233,685 issued to Smith, et al.

Smith teaches a method and apparatus for establishing the provable integrity of a device. Smith does not teach or suggest using a record ID for authentication within a public key system.

Claims 2-4 depend on claim 1, and incorporate its limitations. Similarly, claims 20-22 depend on claim 17 and incorporate its limitations. As discussed above, Cuccia does not teach or suggest looking up a record ID. Smith does not address this feature either. Therefore, Smith does not overcome the shortcomings of Cuccia. Thus, claims 2-4 and 20-22 are patentable over Cuccia in view of Smith.

C. Claims 7, 10, 25 and 28 are Patentable under 35 U.S.C. §103(a) over Cuccia, et al. as applied to claim 1 above, and further in view of U.S. Patent No. 6,581,161 issued to Byford.

Examiner rejected claims 7, 10, 25 and 28 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,151,676 issued to Cuccia, et al. as applied to claim 1 above, and further in view of U.S. Patent No. 6,581,161 issued to Byford.

Byford discusses the use of a portable communication device (i.e. smart card) and providing controlled access to a facility. Byford does not teach or suggest

using a record ID for authentication within a public key system. Therefore, Byford does not overcome the shortcomings of Cuccia.

D. Claims 15, 16, 18 and 21 are Patentable under 35 U.S.C. §103(a) over Cuccia, et al. as applied to claims 14 and 17 above, and further in view of U.S. Patent No. 5,692,106 issued to Towers, et al.

Examiner rejected claims 15, 16, 18 and 21 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,151,676 issued to Cuccia, et al. as applied to claims 14 and 17 above, and further in view of U.S. Patent No. 5,692,106 issued to Towers, et al.

Towers discusses fault diagnosis and service installation systems in a computer system, using an inference engine. Towers discusses system management.

Appellants respectfully submit that there is no suggestion in either Cuccia or Towers for the combination created by the Examiner. Towers has nothing to do with biometrics, remote authentication, or anything of that sort. Rather, Towers is concerned with scheduling task programs. Therefore, the rejection over the combination of Towers and Cuccia is improper.

Furthermore, Towers does not teach or suggest having an authentication server which receives a policy from a third party server, the policy specifying the authentication methodologies for that server. The Examiner refers to column 13, lines 31-48 of Towers. However, the referenced section of Towers discusses the usage policies associated with a computer system (such as the naming of the home

directory, etc.) Towers' use of the term 'policy' is in no way equivalent to the policy described in claims 15, 16, 18, and 21. The Appellant's terminology should be interpreted in light of the Specification.

Furthermore, Appellants note that in the Final Office Action, the Examiner suggests that Towers discusses determining an authentication policy associated with the user. As is clear from Appellant's Detailed Description, the term "policy" describes the authentication policy of the third party server, rather than the user. (See for example Detailed Description, page 18, lines 4-17).

Claim 21 incorporates the limitations of its parent claim, and thus also recites "receiving a record ID." Towers does not teach or suggest the use of such a record ID. Therefore, for at least the reasons discussed above Cuccia in view of Towers does not anticipate claim 21.

D2. Claims 15-16

The Examiner rejected claims 15-16 over the combination of Cuccia and Towers. Claims 15-16 depend on claim 14, and incorporate its limitations. As noted above, neither Cuccia nor Towers teach or suggest third party server looking up a record ID associated with the user. Therefore, claims 15-16 are not obvious over Cuccia in view of Towers.

D3. Claim 18

The Examiner rejected claim 18 over the combination of Cuccia and Towers. Claim 18 depends on claim 17, and incorporates its limitations. As noted above,

neither Cuccia nor Towers teach or suggest the use of a record ID, recited in claim 17. Furthermore, claim 18 recites:

The system of claim 17, further comprising:
a policy validation logic to receive a policy from the third party server,
and determine if the policy has been fulfilled; and
the decryption logic to decrypt the one-time key only if the policy has
been fulfilled.

Cuccia does not teach or suggest a policy validation logic to receive a policy from the third party server. In fact, Cuccia does not teach or suggest the use of a third party server in connection with the authentication function. As noted above Towers also does not teach or suggest receiving a policy from the third party server. Rather, Towers suggests retrieving a user-associated policy from within the same server. This is in no way equivalent to receiving a policy from the third party server.

Therefore, claim 18 is not obvious over the combination of Cuccia and Towers.

E. Claims 19 and 22 are Patentable under 35 U.S.C. §103(a) Cuccia, et al. as applied to claim 17 above, and further in view of U.S. Patent No. 6,119,227 issued to Mao.

Examiner rejected claims 19 and 22 under 35 U.S.C. §103(a) as being unpatentable over Cuccia, et al. and further in view of U.S. Patent No. 6,119,227 issued to Mao.

Mao discusses authentication by an intermediary. However, Mao does not teach or suggest using a record ID for authentication within a public key system. Claims 19 and 22 depend on claim 17, and incorporate its limitations. As discussed

above, Cuccia does not teach or suggest “an authentication server to receive a record ID for a user, and a one-time key generated by a third party server and encrypted with a user’s public key by the third party server.” Mao does not cure the shortcomings of Cuccia. Therefore, Appellants respectfully submit that claims 19 and 22 are not obvious over Cuccia in combination with Mao.

VIII. CONCLUSION

Appellant submits that the references cited by the Examiner do not anticipate or make obvious the claims as they presently stand. Cuccia discusses authentication between a server and a client, but fails to teach or suggest the use of record IDs associated with third party servers. Similarly, the other references, Smith, Byford, Towers, and Mao fail to teach or suggest such a use of a record ID. Furthermore, none of the references teach or suggest the use of a partner key, third party server looking up a record ID, and enabling policy validation.


Appellant respectfully submits that all the appealed claims in this application are patentable and requests that the Board of Patent Appeals and Interferences overrule the Examiner and direct allowance of the rejected claims.

This brief is submitted with a check for \$500.00 to cover the appeal fee for one other than a small entity as specified in 37 C.F.R. § 1.17(f).

Please charge any shortages and credit any overcharges to our Deposit Account No. 02-2666.

Respectfully submitted,
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Date: 1/18, 2005



Judith A. Szepesi
Attorney for Appellants
Registration Number: 39,393

12400 Wilshire Boulevard, Seventh Floor,
Los Angeles, CA 90025-1026
(408) 720-8300

IX. Appendix of claims

1. (Previously Presented) A method of authenticating a client, the method comprising in an authentication server:

receiving a record ID for a user, and a one-time key generated by a third party server and encrypted with a user's public key by the server;
receiving the user's authentication data from the client;
determining if the user's authentication data matches the record ID; and
if so, decrypting the one-time key with the user's private key, and returning the decrypted one-time key to the client.

2. (Previously Presented) The method of claim 1, further comprising registering the user with the authentication server, registering comprising:

receiving a registration authentication data from the user;
generating a random public key/private key pair for the user;
generating a random record ID for the user; and
associating the authentication data and the private key with the record ID.

3. (Original) The method of claim 2, further comprising:
sending the record ID and the public key to the user.

4. (Previously Presented) The method of claim 2 further comprising establishing a secure connection between the authentication server and the user, prior to receiving registration authentication data.

5. (Previously Presented) The method of claim 1, wherein a web page presented by the third party server to the client prompts the user to enter the authentication data to log in to the server.

6. (Original) The method of claim 5, wherein the client's authentication data is automatically redirected to the authentication server.

7. (Original) The method of claim 1, wherein the authentication data is biometric data.

8. (Original) The method of claim 1, wherein the authentication data is personal data selected from among the following: a password, a smart card, and another type of authentication card.

9. (Previously Presented) The method of claim 1, wherein the client forwards the decrypted one-time key to the third party server, thereby authenticating the user as the owner of the private key.

10. (Original) A method of claim 1, further comprising discarding the record ID after returning the one-time key to the user.

11. (Original) The method of claim 1, wherein the record ID and the encrypted one-time key are further encrypted using a partner key, the method further comprising decrypting the record ID and encrypted one-time key using the partner key.

12. (Original) The method of claim 11, wherein the partner is a symmetric key set up during registration of the partner.

13. (Original) The method of claim 11, wherein the partner key is a private key of the authentication server.

14. (Previously Presented) A method of using an authentication server to authenticate a user to a third party server, the method comprising the third party server:

looking up a record ID associated with the user;
generating a one-time key and encrypting the one-time key with a public key of the user, and sending the encrypted one-time key and the record ID to the user;
receiving authentication data, the authentication data being the decrypted one-time key decrypted with the user's private key by the authentication server, such that the user does not have control of the user's private key at any time; and
permitting access to the server.

15. (Original) The method of claim 14, comprising:
determining an authentication policy associated with the user; and
verifying that the authentication policy has been satisfied, prior to permitting access to the server.

16. (Original) The method of claim 15, wherein verifying that the authentication policy has been satisfied comprises:

determining if the server should verify additional data; and
if so, requesting additional data from the user prior to generating the one-time key.

17. (Previously Presented) A third-party authentication system comprising:

an authentication server to receive a record ID for a user, and a one-time key generated by a third party server and encrypted with a user's public key by the third party server;

a comparison logic in the authentication server to receive user authentication data from the client and determine whether the user's authentication data matches the record ID; and

a decryption logic in the authentication server to decrypt the one-time key with a private key associated with the validated record ID, and to return the decrypted one-time key to the client.

18. (Previously Presented) The system of claim 17, further comprising:
a policy validation logic to receive a policy from the third party server, and determine if the policy has been fulfilled; and

the decryption logic to decrypt the one-time key only if the policy has been fulfilled.

19. (Original) The system of claim 17, further comprising:
a nonce generation logic to generate a nonce, the nonce to be included with the user authentication data from the client; and

the comparison logic to verify that the user authentication data includes the appropriate nonce.

20. (Original) The system of claim 17, further comprising a client registration logic to register the user, the client registration logic comprising:

a key generation logic to generate a random public key/private key pair for the user;

a record ID generation logic to generate a random record ID for the user; and

the client registration logic to associate user authentication data with the private key and the record ID.

21. (Original) The system of claim 18, further comprising:
the interface to send the record ID and the public key to the user.

22. (Original) The system of claim 19, wherein the interface establish a secure connection with the user, prior to receiving registration authentication data.

23. (Original) The system of claim 17, wherein a web page presented by the server to the client prompts the user to enter the authentication data to log in to the server.

24. (Original) The system of claim 23, wherein the client's authentication data is automatically redirected to the authentication server.

25. (Original) The system of claim 17, wherein the authentication data is biometric data.
26. (Original) The system of claim 17, wherein the authentication data is personal data selected from among the following: a password, a smart card, and another type of authentication card.
27. (Original) The system of claim 17, wherein the client forwards the decrypted one-time key to the server, thereby authenticating the user as the owner of the private key.
28. (Original) The system of claim 17, further comprising a security mechanism to discard the record ID after returning the one-time key to the user.
29. (Original) The system of claim 17, wherein the decryption logic further decrypts the record ID and the encrypted one-time key with a partner key.
30. (Original) The system of claim 29, wherein the partner key is a symmetric key set up during registration of the partner.
31. (Original) The system of claim 29, wherein the partner key is a private key of the authentication server.